

A Metadata-based Need-to-Know Engine as Part of Standard Content Management Software

**Bruce Lownsbery, Deputy Project Leader
LLNL's Nuclear Weapons Information Project
Presented at InterLab 2000, November 1, 2000**



**Work performed under the auspices of the U.S. Department of Energy by
Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.**

Outline



- **Overview**
- **Background on the NWC NTK effort**
- **NTK Access Control Modes**
- **Xpedio Product Overview and Architecture**
- **Xpedio Standard 'Structured-Mode'**
- **Xpedio Metadata-based NTK Implementation**
- **Xpedio NTK DEMO**

NWC NTK Vision and Architecture



Within DOE's Nuclear Weapons Complex, we want seamless and ubiquitous access (or denial) to information based on the information content and user's credentials

Implemented as distributed but compatible services to:

- Authenticate users and processes
- Validate authorization to resources
- Deliver information securely
- Audit NTK processes

Progress



- **DOE's NWC has worked NTK issues for several years**
 - NWC NTK Architecture approved as good general approach
 - Lots of debate over granularity required and access modes
 - Was no commercial option so NTK Engine prototype developed at LLNL
- **LLNL requested “metadata-based” NTK in product**
 - IntraNet Solutions caught our vision and implemented NTK as add-on when we bought another copy of Xpedio product at list price (\$150K).
 - Prototype delivered in <4 months – took 3 more to become released product in June 2000. Ongoing development.
 - Developed product module is free to all US Government organizations



NTK Access Control Modes

- **Discretionary access**

User determines if a recipient has proper need-to-know
Implemented with personal transfer of information

- **Structured access**

Need-to-know “predefined” by resource owner –
bins of users and content

Implemented by groups, accounts, access control lists, partitioned network connections

- **Content-based access**

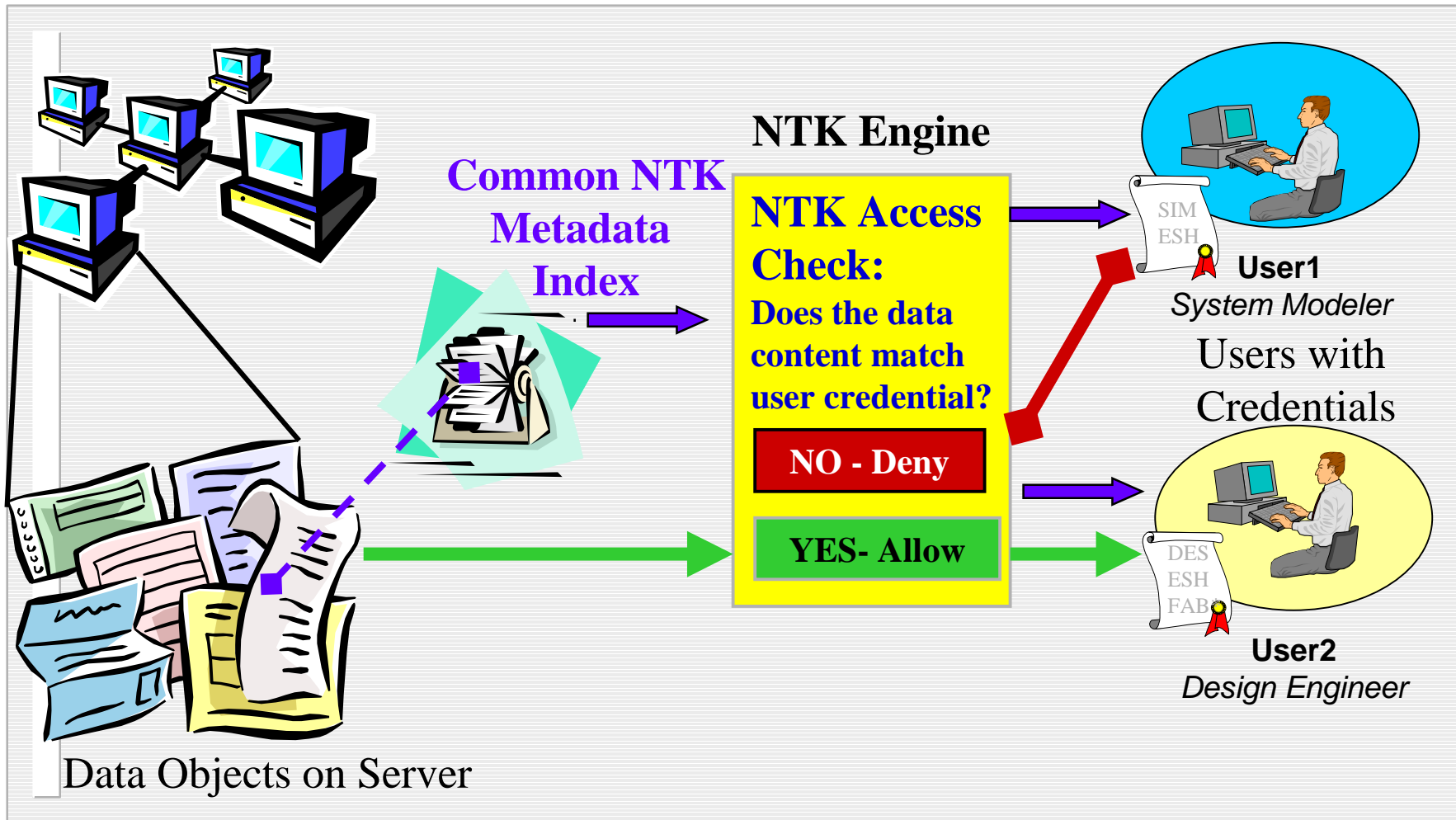
NTK defined by user’s credential and metadata characterizing content
LLNL NTK engine prototype matches certain fields

IntraNet Solutions' Implementation



- **Extend structured mode to metadata-based access in Xpedio Content Server**
- NTK defined by user's credential and metadata characterizing the content
- Commercial NTK Engine runs arbitrarily complex queries
- **Integrated end-to-end solution for:**
metadata, content, and user credential management
with search and browse access in a WWW environment
imposing flexible and powerful NTK control
- Potential front-end for other back-end data repositories and externally managed user credentials

Metadata-based NTK Mechanism (Generalizing Content-based NTK)



Xpedio Metadata and Document Management



NWIP

**Role-based Security
(Structured mode)**

NWIP Internal Use
Security group is nwip

NWIP Presentations

NWIP Documents

NWIP Test Directory

Computer Security Information

Intranet Solutions Tech

Administration Applets for nwipnt



Web Layout Editor



User Admin



Document Manager



Archiver



Workflow



Document Configuration

**Hierarchical
WWW structure
for browse and
also full-content
search of documents
and metadata**

**Query based assignment of documents
to contexts with automatic publishing to WWW**

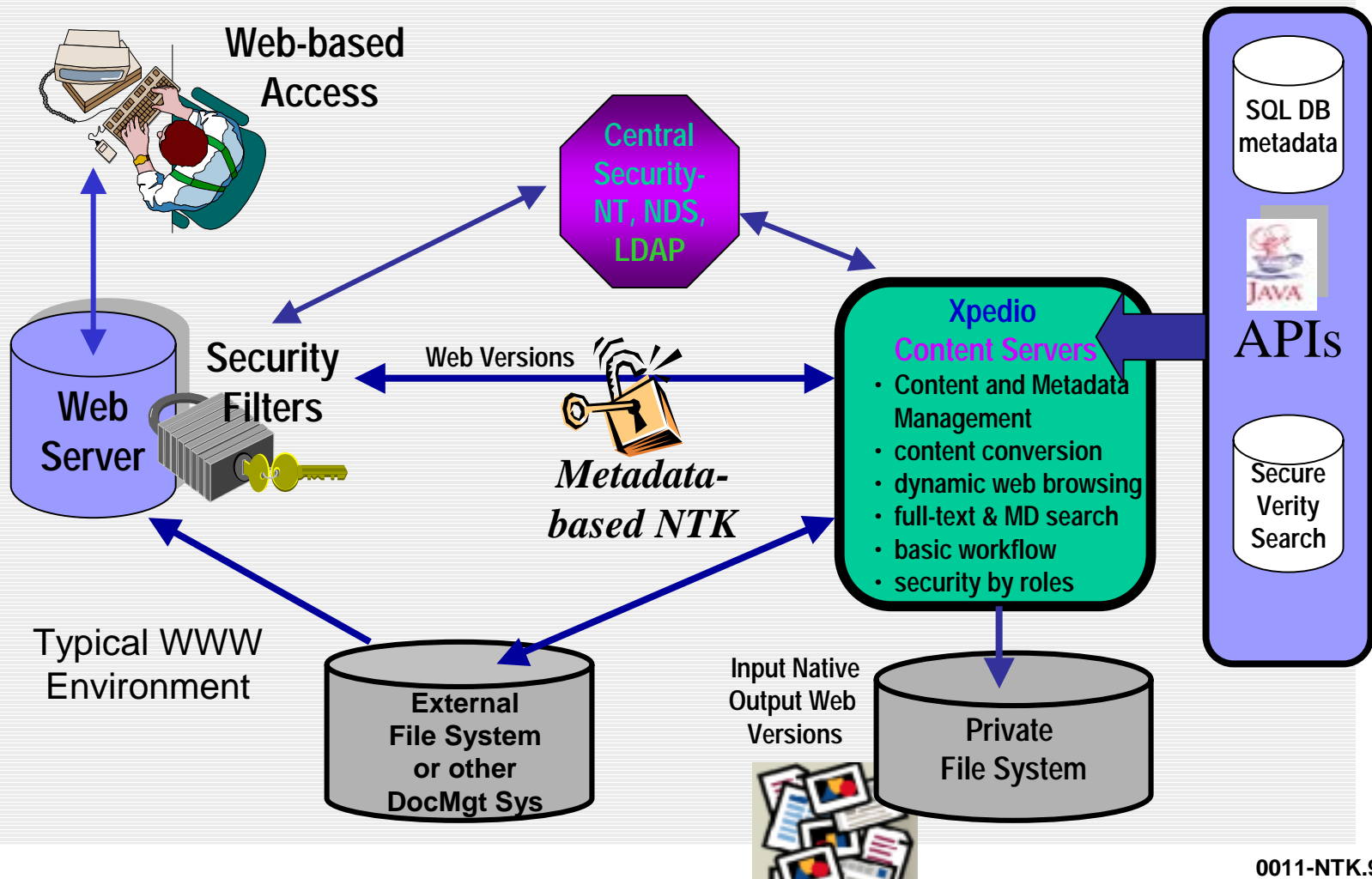
The screenshot displays the NWIP web interface. At the top, it says "NWIP Protecting the future, by preserving the past" with navigation buttons: BACK, HOME, DOCMAN, SEARCH, and HELP. Below this, a search query "Computer Security Information" is shown, with the result "Keywords contain Computer Security". A table lists 8 documents matching the query:

	Revisions	Info	CheckOut
Classification manual MANUAL OF AIS SECURITY REQUIREMENTS	1	1	✓
C932114 SGI IRIX 6.X testing	1	1	✓
C932119 Windows NT 4.x Testing	1	1	✓
C932122 Netscape Enterprise 3.x Web Server Testing	1	1	✓
DOE-5610-2 CONTROL OF WEAPON DATA	1	1	✓
DOE-M5632-1C-1 PROTECTION AND CONTROL OF	1	1	✓

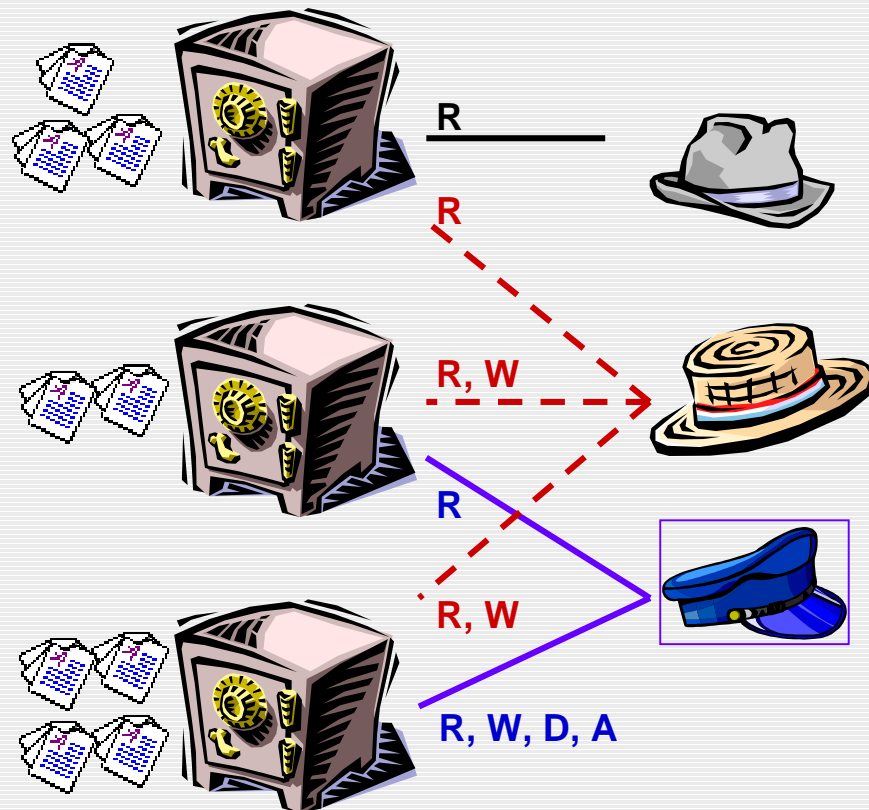
Below the table, there are two overlapping windows. The "Web Layout Editor" window shows a "Web Page Hierarchy" tree with nodes: index, ADAPPhone, OnlineHelp, and nwipnt.html. The "Query Link Definition" window shows "Link Properties" with "Link Title" as "Computer Security Information" and "Description" as "Computer Security Information". The "Query Definition" section shows a query expression: "keywords AND Subjecting computer security".

**JAVA based administration -
including WWW layout
and metadata configuration**

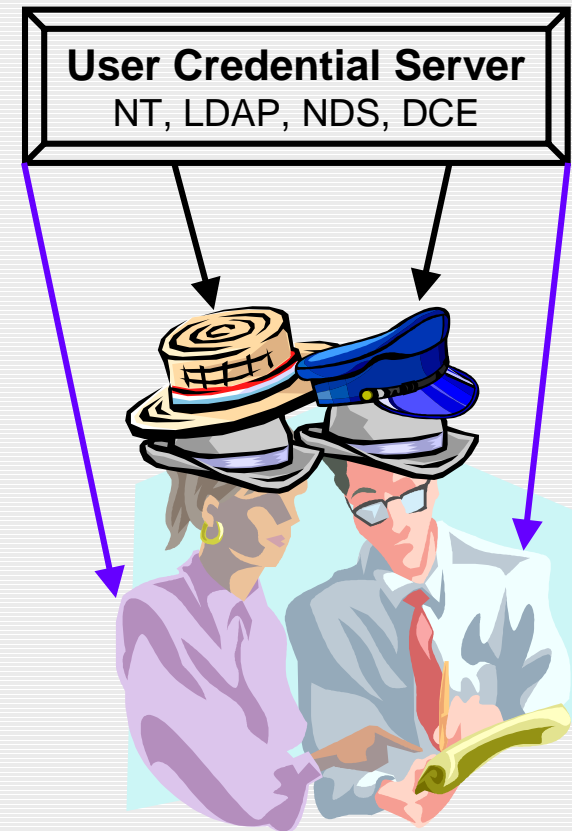
Existing Xpedio Architecture Readily Incorporated NTK Control



Xpedio Standard 'Structured-Mode'



- Documents assigned to 1 Security Group
- Roles have various permissions on Groups
- Users assigned 1 or more Roles
(may be mapped from external credentials)



Xpedio Metadata-based NTK Implementation



- **Functionality and GUI changes implemented with add-on ‘component’**
 - Externally defined fields for access control check between user and content
 - *Demo will use: NTK_Organization, Category, Caveats, and Sigmas along with Usernames and/or Roles to control access*
 - Changes GUI for user credential and GUI for metadata entry
 - Installs in minutes. Disabling reverts to standard structured mode
- **Subset of metadata for selected security groups shown to all users**
 - Metadata subset controlled by search results template
 - GUI for selecting groups for metadata exposure
 - *Implemented via read privilege for ‘hitlist’ role*
- **NTK Query applied only to specified groups**
 - Configuration files identifies applicable security groups
 - NTK query stored in database field – could be interactive or computed
 - GUI for specifying simple queries – then fully editable
 - Null query defaults to standard security for smooth transition
 - Can expand or restrict Read access (doesn’t affect those with Write privilege)
- **Changes to access are nearly instantaneous**

Xpedio User Admin Extended With NTK Fields



User Admin

Users Aliases

☒ Use Filter

Users:

User Name	Full Name	E-Mail Address	NTK_Org	Category	Caveats	Sigma
bel	Bruce Lowensbery	bel@nl.gov	LL-B	SPM, IM		15
bookless1	Bill Bookless	bookless1@nl.gov	LL-DNT	SPM		15
guest						
lowensbery1	Bruce Lowensbery	lowensbery1@nl.gov	LL-B	ND,CMS,ENG, IM	_LLNL_ONLY,NOFORN...	15
miller1	Charlie Miller	cmiller@nl.gov	LA-X	ND, IM	NOFORN	
schwab1	Mike Schwab	schwab1@nl.gov	LL-W	ENG, IM	_LLNL_ONLY,NOFORN	
sysadmin	Bruce Lowensbery	lowensbery1@nl.gov				

Custom NTK Fields

- UI provides simple tool to specify entries in custom fields
- Tool automatically updates based on externally defined custom fields

Ready

Warning: Applet Window

Show Columns

- ☒ User Name
- ☒ Full Name
- ☐ User Type
- ☐ Auth Type
- ☒ E-Mail Address
- ☒ NTK_Org
- ☒ Category
- ☒ Caveats
- ☒ Sigma
- ☐ Organization
- ☐ Source
- ☐ Save Settings

Warning: Applet Window

Xpedio Metadata Entry Extended With NTK Specification Applet



Back | Home | Library | Search | Help

Info Update

Content ID	LL-NWIP-000436
Type	Document
Title	NWIP FY00 Strateg
Author	bel
Security Group	NWIP
Revision	1a
Other IDs	
DocDisclosureQuery	(stdSecurity or (UserName like 'schwab1') or (uNTK_Org like 'LL-DNT LL-W') and (uCategory like 'SPM'))
Docauthor	Lownsbery, BE; Bookless, WA
Project	NWIP
Keywords	Archiving Strategy; Budget Proposals
Archive	No

Warning: Applet Window

Disclosure Query Security

Query Definition

Field: Category

Operator: Is

Value: SPM

Query Expression

User Name Is schwab1
NTK_Org Is LL-DNT|LL-W
Category Is SPM

Warning: Applet Window

Append Replace Cancel

Update

- UI provides simple tool to specify NTK queries – fully editable for power user
- UI automatically updates based on externally defined custom fields and choice lists



Xpedio NTK Demo

- **Open user administration to show user credentials**
 - GUI for structured-mode roles and associated group privileges
 - GUI for changing NTK field values
 - GUI for specifying metadata exposure – NWIP group
- **Log in as users with various privilege and see effects**
 - User 'bel' with Administrator privilege for global access
 - User 'lownsbery1' without general read privilege in NWIP group
- **Change metadata exposure and see effect – toggle NWIP group**
- **Change NTK to allow access where previously excluded - via custom field, username, or role combination**
 - Add category 'IM' to lownsbery1 credential and/or
 - Add lownsbery1 and/or 'public' role to document access criteria